



# Department of Homeland Security Daily Open Source Infrastructure Report for 26 June 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](#)

<http://www.dhs.gov/>

## Daily Highlights

- The Associated Press reports copper thefts are rising, leading to dangerous practices; a thief trying to steal copper from an electric substation near Rutland, Vermont, got a jolt of electricity strong enough to leave scorch marks. (See item [2](#))
- eWeek reports five spreadsheet files with personal data — including the names, birth dates, and social security numbers for approximately 28,000 sailors and family members — were found on an open Website. (See item [11](#))
- The Miami Herald reports that according to a federal indictment unsealed on Friday, June 23, the seven men arrested in Miami in an alleged terrorist plot believed they were conspiring with al Qaeda "to levy war against the United States" in attacks that would "be just as good or greater than 9/11." (See item [38](#))

### DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 23, Houston Business Journal* — Anadarko to buy Kerr–McGee, Western Gas for \$21.1B. Anadarko Corp. has inked deals to acquire Kerr–McGee Corp. and Western Gas Resources Inc. in separate deals totaling \$21.1 billion. Kerr–McGee's core properties are

located in the deepwater Gulf of Mexico and onshore in Colorado and Utah. They include 504 deepwater Gulf of Mexico blocks, encompassing seven operated and three non-operated producing fields, three operated and five non-operated discoveries in varying stages of development, and four additional prospects that will be drilled this year. Western Gas Resources year-end 2005 proven reserves totaled 153 million barrels of oil equivalent (BOE), with proved undeveloped reserves representing 57 percent of the total, while 2006 production is expected to total about 12.5 million BOE.

Source: <http://biz.yahoo.com/bizj/060623/1306650.html?.v=1>

2. *June 22, Associated Press* — **Copper thefts rising in Vermont, leading to dangerous practices.** A thief trying to steal copper from a Central Vermont Public Service Corp. (CVPS) electric substation near Rutland, VT on Wednesday, June 21, got a jolt of electricity strong enough to leave scorch marks. The thief cut a number of ground wires attached to fencing, switches, and regulators to take the copper. The thief got an estimated \$60 worth of copper, CVPS said, but the repairs that were required cost \$5,000. The company learned of the incident when a commercial customer complained that its voltage had dropped. Thieves increasingly have been stealing copper across the country as its prices rises. The grounding wire, for example, can be sold for scrap and recycling at almost \$4 a pound. That's 2 1/2 times more than what it was commanding a year ago. CVPS issued a joint statement Wednesday, June 21, along with Green Mountain Power Corp. and Vermont Electric Power Co. offering rewards for information about anyone stealing the copper wire.

Source: [http://www.boston.com/news/local/vermont/articles/2006/06/22/copper\\_thefts\\_rising\\_in\\_rutland\\_leading\\_to\\_dangerous\\_practices/](http://www.boston.com/news/local/vermont/articles/2006/06/22/copper_thefts_rising_in_rutland_leading_to_dangerous_practices/)

3. *June 22, Associated Press* — **Green Mountain Power to be acquired by Quebec company.** Green Mountain Power announced Thursday, June 22, that it was being acquired by the subsidiary of a Quebec company that operates natural gas transmission and distribution companies elsewhere in northern New England. The deal with Northern New England Energy Corp. was valued at \$187 million in cash. Northern New England Energy currently owns Vermont Gas Systems based in South Burlington and Portland Natural Gas Transmission Systems based in Portsmouth, NH. Northern New England Energy is a subsidiary of Gaz Metro Limited Partnership based in Montreal. Green Mountain Power is in the midst of searching for new energy supplies because its biggest sources — supplied through long-term contracts with the Hydro-Quebec utility in Montreal and the Vermont Yankee nuclear power plant — are expiring over the next decade.

Source: <http://business.bostonherald.com/businessNews/view.bg?articleid=145016>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

4. *June 24, Daily Advertiser (LA)* — **Diesel spill in Louisiana snarls traffic.** A diesel spill near the intersection of University Avenue and Interstate 10 in Lafayette, LA, on Friday afternoon, June 23, led to the arrest of two men suspected of stealing a truck. The spill snarled traffic on the roadway for about an hour. The spill at I-10 and University was the second spill of the day. The first spill happened around noon at the intersection of Willow Street and Evangeline Thruway.

Source: <http://www.theadvertiser.com/apps/pbcs.dll/article?AID=/2006/0624/NEWS01/606240317/1002>

5. *June 23, KNOE TV 8 (LA)* — **Fire at plant in Louisiana prompts evacuations.** Seven hundred employees of Pilgrim's Pride Processing Plant in Farmerville, LA, were evacuated after a fire broke out Friday, June 23. The area the fire was located is the area where live chickens are received before they are slaughtered then processed. Union Parish officials also evacuated residents living within a one-mile radius of the plant due to the concern of fumes from hazardous materials being released into the air.

Source: <http://www.knoe.com/fullstory.php?id=1735>

[[Return to top](#)]

## **Defense Industrial Base Sector**

6. *June 22, Government Accountability Office* — **GAO-06-905T: Information Technology: VA and DoD Face Challenges in Completing Key Efforts (Report).** The Department of Veterans Affairs (VA) is engaged in an ongoing effort to share electronic medical information with the Department of Defense (DoD), which is important in helping to ensure high-quality health care for active duty military personnel and veterans. Also important, in the face of current military responses to national and foreign crises, is ensuring effective and efficient delivery of veterans' benefits, which is the focus of VA's development of the Veterans Service Network (VETSNET), a modernized system to support benefits payment processes. The Government Accountability Office (GAO) is testifying on (1) VA's efforts to exchange medical information with DoD, including both near-term initiatives involving existing systems and the longer term program to exchange data between the departments' new health information systems, and (2) VA's ongoing project to develop VETSNET. To develop this testimony, GAO relied on its previous work and followed up on agency actions to respond to GAO recommendations. GAO has previously made numerous recommendations on these topics, including that VA and DoD develop an integrated project plan to guide their efforts to share patient health data, and that VA develop an integrated project plan for VETSNET.

Highlights: <http://www.gao.gov/highlights/d06905thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-905T>

[[Return to top](#)]

## **Banking and Finance Sector**

7. *June 23, Finextra* — **Police arrest Canadian card cloning gang.** Police in Montreal have arrested nine people that allegedly used rigged payment terminals to skim debit cards and steal customer's PINs. The gang is thought to have stolen millions of dollars from 18,000 customer bank accounts. The criminals targeted convenience stores and petrol stations and bribed shop staff to install fake payment terminals which skimmed debit cards and recorded PINs. Local press reports say the gang included a call center employee who worked for a subcontractor to French bank Mouvements Desjardins and is alleged to have sold customer data to the scammers, such as dates of births.

Source: <http://finextra.com/fullstory.asp?id=15490>

8. *June 23, VNUNet* — **Phisher gets 21-month jail term.** A 23-year-old phishing site operator from Iowa has been sentenced to 21 months in jail and will have to pay \$57,294 in restitution. Jayson Harris had pleaded guilty to two counts of wire fraud and fraud. Harris operated a bogus MSN billing Website between January 2003 and June 2004, guiding visitors to the site through spam e-mail messages. The e-mails asked MSN customers to visit the Website and update their account information and credit card numbers in exchange for a 50 percent discount for the next month's MSN service. Microsoft tracked down the phisher and forwarded the information to the FBI. Microsoft is known for hunting down online criminals, but its actions have mostly resulted in the arrest and conviction of botnet operators. The Harris case is the first time that the company has assisted in the conviction of a phisher.

Source: <http://www.vnunet.com/vnunet/news/2158925/phishing-site-operator-gets-21>

9. *June 23, Websense Security Labs* — **Phishing Alert: Santa Barbara Trust (Voice Phishing).** Websense Security Labs has received reports of a new phishing attack that targets customers of Santa Barbara Bank & Trust in California. Users receive an e-mail message that is spoofed and has the subject "Message 156984 Client's Details Confirmation (Santa Barbara Bank & Trust)." Unlike the most popular form of phishing where users are lured to click on a URL and are directed to a fraudulent site, this lure uses a telephone number. The phone number is in the Southern California area code. When victims dial the phone number, the recording requests that they enter their account number. The phone response does not mention the bank name, which could be a potential indicator that this number is being used for fraud against other entities.

Recording link: [http://www.websense.com/securitylabs/images/alerts/june\\_vishing.wav](http://www.websense.com/securitylabs/images/alerts/june_vishing.wav)

Source: <http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=534>

10. *June 23,* — **Florida banks, U.S. Treasury conduct pandemic-response drill.** The U.S. Treasury Department Friday, June 23, helped South Florida banks conduct the first-ever test of financial systems should a flu pandemic hit the country. The Treasury Department and FloridaFirst conducted the drill at the Miami-Dade Emergency Operations Center. FloridaFirst's goal is to prepare financial institutions to respond to threats or events caused by terrorism or natural disasters. Treasury spokesperson Jennifer Zuccarelli said the department hopes the exercise will encourage other regions across the country to conduct similar drills.

Source: <http://www.miami.com/mld/miamiherald/14877474.htm>

11. *June 23, eWeek* — **U.S. Navy: data breach affects 28,000.** Five spreadsheet files with personal data on approximately 28,000 sailors and family members were found on an open Website, the U.S. Navy announced Friday, June 23. The personal data included the name, birth date, and social security number on several Navy members and dependents. The Navy said it was notified on June 22 of the breach and is working to identify and notify the individuals affected. "There is no evidence that any of the data has been used illegally," the Navy said. Individuals affected by the breach will be contacted soon to ensure they have information on how to guard against identity theft. The files have been removed from the site, and Navy's chief of personnel is working with the law enforcement to determine how and when the files were placed on the Web and prevent future release of information of this type.

Source: <http://www.eweek.com/article2/0.1895.1981041.00.asp>

12. *June 23, eWeek* — **Cyber criminals use P2P tools for identity.** Cyber criminals are multiplying quickly and becoming more sophisticated in the ways in which they take advantage of unwitting Internet individual users and companies, said Howard Schmidt, a co-architect of the national cyber-security policy presented to the president's Critical Infrastructure Protection Board in 2003. At an SD Forum seminar Thursday, June 22 Schmidt said Peer-to-peer (P2P) networks such as Limewire, Kazaa, Grokster, and others aren't helping to quell the increase in crimes committed via the Internet. The Internet cultivates careless and ignorant use of P2P applications as a major part of the current identity theft problem. People who use P2P applications to download music, software, and photos may leave themselves wide open to identity theft by simply being unaware of their computer settings. "One woman's credit-card information was found in such disparate places as Troy, MI, Tobago, and Slovenia. Why? We found that the "shared" folder in her music-downloading application was in fact making readily available her entire "My Documents" folder to that app's entire P2P audience, 24 hours per day," Schmidt said. By typing in common search terms such as "bank May statement," or "stop payment" in Limewire's search function, personal information is often getting into the wrong hands, enabling cyber-looting.  
Source: <http://www.eweek.com/article2/0,1895,1980963,00.asp>

13. *June 22, Federal Trade Commission* — **FTC notifies individuals of theft.** The Federal Trade Commission (FTC) on Thursday, June 22, announced it is notifying approximately 110 individuals that two FTC laptop computers, one of which contained some of their personally identifiable information, were stolen from a locked vehicle. The FTC has no reason to believe the information on the laptops, as opposed to the laptops themselves, was the target of the theft, said the release. In addition, the stolen laptops were password protected and the personal information was a very small part of several thousand files contained in one of the laptops. The personal information was gathered in law enforcement investigations and included, variously, names, addresses, Social Security numbers, dates of birth, and in some instances, financial account numbers. The FTC will offer these individuals one year of free credit monitoring. The FTC's inspector general is investigating the theft.  
Source: [http://www.govtech.net/magazine/channel\\_story.php/99964](http://www.govtech.net/magazine/channel_story.php/99964)

14. *June 22, Durham Region (NC)* — **Police break card-skimming scam.** Four men have been charged after Durham, NC, police identified what they're describing as a large-scale counterfeit operation that targeted debit card users at a Pickering restaurant. Hundreds of blank plastic smart cards, skimming equipment and a number of pinhole cameras were seized as a result of the investigation by fraud officers, who set up surveillance after receiving information about the scam Monday, June 19. With the assistance of an employee, the scammers rigged a debit payment machine to record information from cards that was stored on a chip. They also concealed a pinhole camera in the ceiling that recorded victims as they entered the PIN number to make purchases, said Detective Constable Jeff Caplan. But police broke up the scam — which they estimate ran for up to three weeks — before the information could be used to create new debit and credit cards, he said. "One major bank had 350 cards compromised...The losses could have been in the millions," Caplan said.  
Source: [http://www.durhamregion.com/dr/regions/top\\_stories/story/3561061p-4114718c.html](http://www.durhamregion.com/dr/regions/top_stories/story/3561061p-4114718c.html)

[[Return to top](#)]

## **Transportation and Border Security Sector**

15. *June 25, Associated Press* — **Flight diverted to JFK after altercation.** Police detained one woman and questioned two others early Sunday, June 25, after a fight broke out in the first minutes of a flight to Puerto Rico, causing the plane to be diverted to John F. Kennedy International Airport (JFK), officials said. One woman apparently started a fistfight with the other two, said Steve Coleman, a spokesperson for the Port Authority of New York and New Jersey, which runs the region's airports. JetBlue Flight 561 with 147 passengers and six crewmembers took off from Newark, NJ. at 12:01 a.m. EDT Sunday and landed at JFK about an hour later, said airline spokesperson Jenny Dervin.  
Source: [http://www.usatoday.com/news/nation/2006-06-25-plane-diverte\\_d\\_x.htm](http://www.usatoday.com/news/nation/2006-06-25-plane-diverte_d_x.htm)
16. *June 25, Associated Press* — **Philadelphia airport briefly evacuated.** Philadelphia International Airport was partially evacuated for about an hour Sunday, June 25, because of a suspicious package, authorities said. About 1,000 people were told to leave while a police bomb squad was brought in to investigate, airport spokesperson Mark Pesce said. The package turned out not to be dangerous, said Pesce.  
Source: [http://hosted.ap.org/dynamic/stories/B/BRF\\_AIRPORT\\_EVACUATION?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/B/BRF_AIRPORT_EVACUATION?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT)
17. *June 23, Government Accountability Office* — **GAO-06-764: Coast Guard: Status of Deepwater Fast Response Cutter Design Efforts (Report).** The Coast Guard has been pursuing a replacement vessel for its aging and deteriorating patrol boats as part of the Integrated Deepwater System (or Deepwater) acquisition. Originally, all 49 of the Coast Guard's 110-foot patrol boats were to be converted into 123-foot patrol boats as a bridging strategy until a replacement vessel, the 140-foot Fast Response Cutter (FRC) came on line beginning in 2018. The initial conversions of the 110-foot patrol boats proved unsuccessful, though, and this prompted the Coast Guard to cancel further patrol boat conversions and accelerate the design and delivery of the FRC from 2018 to 2007. Early design efforts called for the FRC's hull, decks, and bulkheads to be made from composite materials rather than steel. Recently, design problems with the FRC's hull shape and weight have raised questions about the viability of the FRC design and use of composite materials. This report examines (1) the factors that went into the decision to use composite materials for the FRC hull, (2) the types of composite materials that have been selected for the FRC hull, (3) the extent of contingency plans developed for use if the prototype hull fails to meet Coast Guard performance requirements, and (4) the status of design efforts for the FRC. The Coast Guard concurred with the findings in this report.  
Highlights: <http://www.gao.gov/highlights/d06764high.pdf>  
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-764>
18. *June 23, Associated Press* — **Great Plains Airlines equipment sold at auction.** Spare parts from liquidated Great Plains Airlines have been sold at an auction to a German company for \$285,000, marking a final chapter in the downfall of a regional carrier that planned to fly directly from Oklahoma City and Tulsa to the East and West Coasts. Great Plains was launched in April 2001 with \$57 million in tax credits and government-backed loans. It filed for bankruptcy reorganization in January 2004 and went through liquidation in 2005 after executives said efforts to find financing and investors had been unsuccessful. Private Wings Flugcharter, a Berlin-based airline that offers business charter and freight services, submitted

the winning bid of \$285,000 at an auction conducted Wednesday, June 21, by U.S. Bankruptcy Judge Terrence Michael.

Source: [http://www.usatoday.com/travel/news/2006-06-22-great-plains-sale\\_x.htm](http://www.usatoday.com/travel/news/2006-06-22-great-plains-sale_x.htm)

19. *June 23, New York Times* — **Verizon to end service on commercial airplanes.** Verizon Airfone, whose handsets have graced the backs of airline seats for more than two decades, will shut down its phone service on commercial airliners before the end of the year. Verizon Communications, Airfone's parent company, has decided instead to focus on its faster-growing broadband, cellular and television businesses, Jim Pilcher, the director of marketing at Verizon Airfone, said. Airfone, which Verizon acquired when it bought GTE in 2000, has phones in about 1,000 planes operated by Continental, Delta, United Airlines and US Airways. The company will work with the airlines to figure out how to remove the phones and other equipment from the planes. Airfone, which began service 21 years ago, will continue to provide telecommunications services on about 3,400 corporate and government planes.

Source: <http://www.nytimes.com/2006/06/23/technology/23cnd-airfone.html?ei=5094&en=1b72e251fc655da5&hp=&ex=1151121600&adxnnl=1&partner=homepage&adxnnlx=1151090656-I7ivsjiOrUistUkUcAoEBQ>

20. *June 23, Department of Homeland Security* — **Border Patrol Academy plans to train 6,000 new agents.** The Border Patrol Academy of U.S. Customs and Border Protection is working with the Federal Law Enforcement Training Center to plan the expansion of training for 6,000 new border patrol agents by the end of 2008. The Border Patrol Academy curriculum is a 91-day, 747-hour program covering five subject areas: Operations, Spanish, Physical Techniques, Driver Training, and Firearms. The initiative to train 6,000 Border Patrol Agents will begin October 1, 2006 (Fiscal Year 2007).

Information on the Border Patrol Academy:

[http://www.cbp.gov/xp/cgov/careers/customs\\_careers/border\\_careers/bp\\_academy/](http://www.cbp.gov/xp/cgov/careers/customs_careers/border_careers/bp_academy/)

Source: <http://www.dhs.gov/dhspublic/>

21. *June 21, Department of Transportation* — **Three airlines proposed for new U.S.–Mexico service.** The Department of Transportation on Wednesday, June 21, proposed to select Delta Air Lines, Frontier Airlines, and JetBlue Airways to provide new service between the United States and Mexico. The new services were made possible by amendments to the U.S.–Mexico air services agreement signed last December. In the show-cause order, the Department tentatively selected Delta for service between Los Angeles and Puerto Vallarta, Frontier for service between Los Angeles and San Jose del Cabo, and JetBlue for New York–Cancun service. Under a show-cause order, interested parties have an opportunity to file objections to the tentative decision before a final decision is made. The liberalized U.S.–Mexico aviation agreement provides that three airlines from each country may fly between any U.S. city and Acapulco, Cancun, Cozumel, Huatulco, Ixtapa/Zihuatanejo, Loreto, Manzanillo, Mazatlan, Merida, Oaxaca, Puerto Vallarta, and San Jose del Cabo.

The show-cause order, carrier filings, and comments: <http://dms.dot.gov>.

Source: <http://www.dot.gov/affairs/dot7306.htm>

22. *June 19, Government Accountability Office* — **GAO–06–571: Commercial Aviation: Costs and Major Factors Influencing Infrastructure Changes at U.S. Airports to Accommodate the New A380 Aircraft (Report).** Airbus S.A.S (Airbus), a European aircraft manufacturer,

introduced a new aircraft, the A380 that will be the largest passenger aircraft in the world with expected delivery to its first customers in late 2006. The A380 has a double deck and is expected to seat between 555 and 853 passengers. A freight version of the A380 is scheduled for delivery in 2008. Because of the size of the A380, U.S. airports have to make changes to accommodate the aircraft. This may include widening runways and taxiways, or restructuring gate areas to accommodate the additional passengers. This report examines (1) the costs and nature of the changes U.S. airports are making to their infrastructure to accommodate the A380, (2) the funding sources being used to finance these changes, and (3) the major factors influencing the changes being made. The Federal Aviation Administration and Airbus provided technical comments on the report. Airbus also commented on the 18 airports' cost estimates of the changes being made for the A380 and estimated \$720 million for these changes. Based on the costs airports reported initially and the Government Accountability Office's (GAO) subsequent reconfirmation efforts, GAO did not change the cost estimates provided by the airports.

Highlights: <http://www.gao.gov/highlights/d06571high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-571>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

- 23. *June 22, Atlanta Business Chronicle* — UPS teams up with EPA on new delivery truck.** The Environmental Protection Agency (EPA) on Thursday, June 22, unveiled a new urban delivery vehicle that it developed in partnership with United Parcel Service (UPS) and other companies. In laboratory testing, the EPA's patented hydraulic hybrid diesel technology achieved a 60 to 70 percent improvement in fuel economy and more than a 40 percent reduction in carbon dioxide emissions, compared to a conventional UPS vehicle. The EPA cited tests showing that the technology used in the truck has the potential to dramatically improve the fuel economy of urban vehicles used in applications such as package delivery, shuttle and transit buses, and refuse pick-up.

Source: <http://www.bizjournals.com/atlanta/stories/2006/06/19/daily9.html>

[\[Return to top\]](#)

## **Agriculture Sector**

- 24. *June 24, Agence France-Presse* — China reports new outbreak of foot-and-mouth disease.** China reported a fresh outbreak of foot-and-mouth disease, with 213 head of cattle stricken in the nation's northwestern Gansu province. The cattle began showing symptoms of the illness on June 14, in Gansu's Zhouqu County, the agriculture ministry reported. The entire herd of 380 cattle was culled following the outbreak, while local agriculture officials quarantined and disinfected the farm and the surrounding area, the ministry said. On May 31, the ministry reported a separate outbreak of foot-and-mouth disease in Gansu's Jiaguguan prefecture, while another outbreak was reported in the province in March. The latest outbreak brings to eight the number of foot-and-mouth epidemics to strike China this year. Foot-and-mouth is a severe, highly contagious viral disease affecting cattle, pigs, sheep and

other cloven-hoofed livestock.

Source: [http://news.yahoo.com/s/afp/20060624/hl\\_afp/healthchinafarm\\_060624200006;\\_ylt=AjA9cxhPKc10g8YxZklqPliJOrgF;\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060624/hl_afp/healthchinafarm_060624200006;_ylt=AjA9cxhPKc10g8YxZklqPliJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)

**25. *June 22, North Dakota Ag Connection* — North Dakota reports first anthrax case of year.**

Two head of cattle have died of anthrax, the first cases of the disease reported in North Dakota this year. The cattle came from a herd in Emmons County, southwest of Linton. Dr. Sheldon Malmedal of Linton examined the animals, and forwarded tissues to the Veterinary Diagnostic Laboratory at North Dakota State University which used a polymerase-chain-reaction test to confirm the diagnosis of anthrax. Last year, anthrax cases were confirmed in Barnes, Cass, Cavalier, Dickey, Grand Forks, Griggs, Kidder, LaMoure, McIntosh, Nelson, Ransom, Sargent, Steele, Stutsman, Traill and Walsh counties. More than 500 animals, including cattle, bison, horses, sheep, llamas, and farmed deer and elk, died from the disease.

Source: <http://www.northdakotaagconnection.com/story-state.cfm?Id=461&yr=2006>

[[Return to top](#)]

## **Food Sector**

**26. *June 23, Agence France-Presse* — Children ill from food poisoning in South Korea.** The South Korean government said it was investigating an outbreak of food poisoning in Seoul-area schools that had sickened 1,700 children. The education ministry said students from 25 schools in the capital region had suffered from symptoms including nausea, diarrhea, stomach aches and fever since Friday, June 16. Health officials shut down cafeterias at dozens of schools in the Seoul area. Prime Minister Han Myeong-Sook, chairing a government meeting, called for an investigation of food distributors who supply meals to schools.

Source: [http://news.yahoo.com/s/afp/20060623/hl\\_afp/skoreahealthfood\\_060623171151;\\_ylt=Ava6d76DINf.yP1y90LJlkuJOrgF;\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060623/hl_afp/skoreahealthfood_060623171151;_ylt=Ava6d76DINf.yP1y90LJlkuJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)

**27. *June 22, U.S. Food and Drug Administration* — Horse feed recalled.** Western Stockmen's, Caldwell, a business unit of J.R. Simplot Company, is recalling all Pride Mature Horse feed, Lot number 7701-050306, because it may contain monensin sodium (Rumensin), a drug compound approved for use in some livestock species which can be fatal if fed to horses. Pride Mature Horse feed was distributed by the Western Stockmen's (WSI) store to customers in Caldwell, ID, and to Cowpoke Ranch Supply in Corvallis, MT, and Three Rivers in Lostine, OR. The U.S. Food and Drug Administration and Western Stockmen's are conducting an investigation to determine how Rumensin appeared in some of the feed. At least two horse deaths related to the consumption of this feed are being investigated. Additional illnesses are also being investigated.

Source: [http://www.fda.gov/oc/po/firmrecalls/stockmen06\\_06.html](http://www.fda.gov/oc/po/firmrecalls/stockmen06_06.html)

[[Return to top](#)]

## **Water Sector**

**28. *June 22, U.S. Environmental Protection Agency* — Puerto Rico Aqueduct and Sewer**

**Authority indicted.** The Puerto Rico Aqueduct and Sewer Authority (PRASA) entered into an agreement to plead guilty to an indictment charging 15 felony counts of violating the federal Clean Water Act (CWA) through the illegal discharge of pollutants from nine sanitary wastewater treatment plants and five drinking water treatment plants, the U.S. Justice Department and Environmental Protection Agency (EPA) announced today. Under the plea agreement, PRASA will pay a criminal fine of nine million dollars — the largest fine ever paid by a utility for violating the CWA. In addition, a comprehensive civil settlement was reached between PRASA and the U.S. resolving repeated environmental violations at 61 wastewater treatment plants throughout the Commonwealth. In the civil settlement, PRASA will spend an estimated \$1.7 billion implementing capital improvement projects and other remedial measures at all of its 61 wastewater treatment plants and related collection systems over the next 15 years.

Source: <http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852570180055e350/f120c4f065c8bce685257195006a1831!OpenDocument>

[[Return to top](#)]

## **Public Health Sector**

**29. *June 25, Agence France–Presse* — Hand, foot and mouth disease kills eleventh child in**

**Malaysia.** A two-year-old boy has become the eleventh child to die in an epidemic of hand, foot and mouth disease in Malaysia's eastern state of Sarawak. Deputy Chief Minister George Chan said the boy died on Friday, June 23, but described the death as an isolated case. The state has been battling the outbreak since February and the number of cases had declined in recent months. Chan said the number of new cases had dropped to around 200 to 250 per week since mid-April from between 1,000 and 1,300 cases per week previously. The illness affects mainly infants and young children, causing painful mouth and throat ulcers, fever and blisters on hands and feet.

Source: [http://news.yahoo.com/s/afp/20060625/hl\\_afp/malaysiahealthdisease\\_060625121405](http://news.yahoo.com/s/afp/20060625/hl_afp/malaysiahealthdisease_060625121405)

**30. *June 23, Associated Press* — Tattoo customers in three states get infections.** A superbug seen in prisoners and athletes is also showing up in people who get illegal tattoos, federal health officials said Thursday, June 22. Forty-four tattoo customers in Ohio, Kentucky and Vermont developed skin infections caused by methicillin-resistant *Staphylococcus aureus* (MRSA). The infections occurred in 2004 and 2005, and were traced to 13 unlicensed tattoo artists. Clusters of MRSA cases were seen in Ohio in June 2004, November 2004 and April 2005, involving 33 people. A four-person cluster was reported in Kentucky in May 2005 and a seven-person cluster was in Vermont in August. Ohio, Kentucky and Vermont require licensing for tattoo artists, but all the affected customers went to unlicensed artists.

MRSA information: [http://www.cdc.gov/ncidod/dhqp/ar\\_mrsa\\_ca.html](http://www.cdc.gov/ncidod/dhqp/ar_mrsa_ca.html)

Source: <http://abcnews.go.com/Health/wireStory?id=2110198>

**31. *June 22, Reuters* — Pentagon says vaccine may have killed U.S. soldier.** A panel of armed forces medical experts has found that vaccines required by the military may have killed a 26-year-old Army soldier last year, the Pentagon said on Thursday, June 22. Pfc. Christopher

"Justin" Abston died on December 4 at Fort Bragg, NC, 16 days after getting smallpox and injectable influenza vaccines, officials said. The panel concluded it was "possible" the vaccines were the cause of death. An autopsy showed Abston suffered from an inflammation of the heart muscle, or myocarditis, a condition the smallpox vaccine is known to cause, the Pentagon said. "The panel cautioned that the findings pointing to vaccinations were neither probable nor unlikely, but they do suggest the possibility that the vaccines may have caused Abston's death."

Source: [http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006-06-23T000733Z\\_01\\_N2272318\\_RTRUKOC\\_0\\_US-ARMS-USA-VACCINE.xml&archived=False](http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006-06-23T000733Z_01_N2272318_RTRUKOC_0_US-ARMS-USA-VACCINE.xml&archived=False)

[\[Return to top\]](#)

## **Government Sector**

Nothing to report.

[\[Return to top\]](#)

## **Emergency Services Sector**

32. *June 23, Richmond Times-Dispatch (VA)* — **Guard to have response team.** Virginia's National Guard will soon have a military task force to help state and local governments deal with a catastrophic terrorist attack or natural disaster. The new task force will be able to decontaminate casualties, treat injured victims and rescue people trapped in damaged buildings. The task force is aimed at assisting civilian authorities confronted with the effects of chemical, biological and radiological releases, high explosives and nuclear weapons.  
Source: [http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMSGArticle%2FRTD\\_BasicArticle&c=MGArticle&cid=1149188688180&path=%21news&s=1045855934842](http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMSGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1149188688180&path=%21news&s=1045855934842)

33. *June 21, North Jersey* — **Emergency call system gets little response in New Jersey.** Only about one in 10 residents in Ridgefield, NJ, responded to the borough's new emergency phone notification system during its first test run, underscoring the need for additional communication channels with residents, emergency officials said. The so-called SwiftReach notification system called 1,000 listed phone numbers and delivered a 30-second recorded mock alert during the trial run Saturday, June 10. The message asked residents to push "1" if they understood it. Only about 12 percent did so, results show. However, about 60 percent of the calls were answered, indicating a significant number of residents hung up before listening to the entire message. The test also revealed some of the system's weaknesses. For example, 108, or roughly 10 percent of the numbers dialed were out of service. A reporter's calls to several failed phone numbers also showed some residents do not understand English.  
Source: <http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVFeXk0NSZmZ2JlbDdmN3ZxZWVFRXI5Njk1MTE2OCZ5cmlyeTdmNzE3Zjd2cWVIRUV5eTI>

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

34. *June 23, eWeek* — **Net disaster could paralyze economy, study warns.** America's Internet and cyber infrastructure have become such a critical backbone for the exchange of information, that any major disruption could have significant economic and security repercussions. The report, issued on Friday, June 23, by the Business Roundtable, a group comprised of chief executives of 160 of the country's largest companies, calls on the federal government to set up response plans and establish clear lines of responsibility.  
The full report: <http://www.businessroundtable.org/pdf/20060622002CyberReconF inal6106.pdf>  
Source: <http://www.eweek.com/article2/0,1895,1980979,00.asp>
35. *June 22, Security Focus* — **Mozilla Network Security Services library remote denial-of-service vulnerability.** Network Security Services is susceptible to a remote denial-of-service vulnerability. This issue is due to a memory leak in the library. Analysis: This issue allows remote attackers to consume excessive memory resources on affected computers. This may lead to computer hangs or panics, denying service to legitimate users. Complete list of vulnerable products: <http://www.securityfocus.com/bid/18604/info>  
Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.  
Source: <http://www.securityfocus.com/bid/18604/references>
36. *June 21, CNET News* — **FCC approves new Internet phone taxes.** An estimated four million subscribers to Internet phone services like Vonage could see new fees on their bills under a plan approved Wednesday, June 21, by federal regulators. The Federal Communications Commission (FCC) voted unanimously at its monthly meeting to require all Voice over Internet Protocol (VoIP) services that connect to the public-switched telephone network — as opposed to using peer-to-peer technology, like Skype — to contribute to the Universal Service Fund. The \$7.3 billion fund, which has been a feature of U.S. policy for more than 70 years, subsidizes telephone service in rural and low-income areas. It also runs a controversy-plagued program called E-Rate that provides discounted Internet and phone service to schools and libraries. Right now, only telecommunications services, including wireless, pay phone, traditional telephone and DSL providers, are required to contribute a fixed percentage of their long distance revenue to the multibillion-dollar fund. It had been unclear whether VoIP providers must also pay. The same FCC order would also raise the share that cell phone providers must contribute to the pool, though it was not immediately clear how many consumers would see hikes or how much they would be.  
Source: [http://news.com.com/FCC+approves+new+Internet+phone+taxes/2100-7352\\_3-6086437.html](http://news.com.com/FCC+approves+new+Internet+phone+taxes/2100-7352_3-6086437.html)
37. *June 20, Associated Press* — **Hacker taps into newspaper Websites.** Hackers broke into the Websites of MaineToday.com early Saturday morning, June 17. MaineToday.com operates a Website under its own name as well as Internet sites for the Portland Press Herald, Kennebec Journal and Morning Sentinel. The hackers, who were apparently out of Brazil, managed to find security weaknesses that enabled them to break into the sites.  
Source: <http://www.seacoastonline.com/news/06202006/maine/108355.htm>

## Internet Alert Dashboard

### DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

**US-CERT Operations Center Synopsis:** US-CERT is aware of active exploitation of a new vulnerability in Microsoft Excel. Successful exploitation could allow an attacker to execute arbitrary code with the privileges of the user running Excel. For more information please review the following:

**Technical Cyber Security Alert: TA06-167A**

<http://www.us-cert.gov/cas/techalerts/TA06-167A.html>

**Vulnerability Note: VU#802324** <http://www.kb.cert.org/vuls/id/802324>

We are continuing to investigate this vulnerability. US-CERT recommends the following actions to help mitigate the security risks:

Install anti-virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

Review the workarounds described in Microsoft Security Advisory 921365:

<http://www.microsoft.com/technet/security/advisory/921365.mspx>

US-CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04-010 for more information on working with email attachments: <http://www.us-cert.gov/cas/tips/ST04-010.html>

### FDIC Phishing Scam

US-CERT continues to receive reports of phishing scams that target online users. Recently, the phishing scam targeted the customers of Federal Deposit Insurance Company (FDIC) insured institutions.

Customers of FDIC institutions received a spoofed email message, which claims that their account is in violation of the Patriot Act, and that FDIC insurance has been removed from their account until their identity can be verified. The message provides a link to a malicious web site which prompts users to enter their customer account and identification information.

If you were affected by the FDIC phishing scam, please refer to the FDIC

**Consumer Alert for assistance:**

**<http://www.fdic.gov/consumers/consumer/alerts/phishing.html>**

**US-CERT confirms that the federal agencies including Department of Homeland Security (DHS) mentioned in the fraudulent email have not sent out an email that requests customer account or identification information.**

**US-CERT encourages users to report phishing incidents based on the following guidelines:**

**Federal Agencies should report phishing incidents to US-CERT:**

**[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)**

**Non-federal agencies and other users should report phishing incidents to OnGuard Online, a consortium of Federal Agencies:**

**<http://onguardonline.gov/phishing.html>**

**Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:**

**Do not follow unsolicited web links received in email messages.**

**Contact your financial institution and file a complaint with the Federal Trade Commission (FTC) immediately if you believe your account or financial information has been compromised.**

**[https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z\\_ORG\\_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03)**

**Review FTC's web site on how to protect yourself from identity theft:**

**<http://www.consumer.gov/idtheft/>**

**Review the OnGuard Online practical tips to guard against Internet fraud, secure your computer, and protect your personal information:**

**<http://onguardonline.gov/phishing.html>**

**Refer to the US-CERT Cyber Security Tip on Avoiding Social Engineering and Phishing Attacks: <http://www.us-cert.gov/cas/tips/ST04-014.html>**

**Refer to the CERT Coordination Center document on understanding Spoofed/Forged Email: [http://www.cert.org/tech\\_tips/email\\_spoofing.html](http://www.cert.org/tech_tips/email_spoofing.html)**

## **PHISHING SCAMS**

**US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:**

**Federal Agencies should report phishing incidents to US-CERT.**

[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)

**Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online.**

<http://onguardonline.gov/phishing.html>

#### Current Port Attacks

<b>Top 10 Target Ports</b>	1026 (win-rpc), 25 (smtp), 445 (microsoft-ds), 38566 (---), 24232 (---), 50497 (---), 80 (www), 135 (epmap), 4672 (eMule), 32790 (---) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[[Return to top](#)]

## **General Sector**

**38. *June 23, Miami Herald* — Officials: South Florida "homegrown terrorists" arrested.** The seven men arrested in Miami in an alleged terrorist plot believed they were conspiring with al Qaeda "to levy war against the United States" in attacks that would "be just as good or greater than 9/11," according to a federal indictment unsealed on Friday, June 23. The campaign, which never advanced beyond the discussion stage, would begin with the bombing of the 110-story Sears Tower in Chicago, according to the indictment. The group's leader, identified as Narseal Batiste, allegedly said he wanted to "kill all the devils that we can," the indictment said. The seven were arrested Thursday, June 22, most of them in Liberty City – a section of Miami – according to federal officials. They met repeatedly with a government informant pretending to represent al Qaeda and swore oaths of fidelity to the group, officials said. Authorities emphasized that the public was not in danger. Still, authorities stopped short of saying that every member of the group had been arrested.

Source: <http://www.miami.com/mld/miamiherald/14880185.htm>

[[Return to top](#)]

## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.